IT Unit 3

Topic 1

# Organisations & Data Management

**Protecting valuable data, p 57**

1. Why is it important that stored data is kept secure?

* To keep the integrity of the information of a business, if this data becomes corrupt or is altered by deliberate threats, the business could lose its reputation or even go belly up.

1. What are the 2 types of controls that can protect data?

* Physical security control- Such as having your computers and devices locked away at a secure location/site.
* Software security control- These are things such as having usernames and passwords, backing up and electrical protection etc.

Measures to protect data:

Physical equipment controls include zoned security strategies, barrier techniques and biometrics.

A What is meant by biometrics and what is its advantage as a means of protecting data?

* It’s an automated method of identifying an individual by analysing personal physiological or behavioural characteristics, such as; fingerprint scanning, face and voice recognition, iris scanning etc. Advantages of this are the efficiency of identifying many people at one time such as soccer matches and its extremely effective way of identifying people because of how accurate it is, unlike things like signatures.

1. Backing up
   1. What are the 3 types of backing up?

* Full, Differential and Incremental
  1. List some backup options?

1. Electrical protection
   1. What is the role of a UPS?

* To give power to a computer or device for a short period of time if a blackout or power surge occurs and thus allowing the user to save what they can in that time.

1. Usernames & passwords
   1. What are the characteristics of a good password?

* Mix of alphanumeric
* Upper case and lower case
* More than eight characters
  1. What is the role of access logs, audit trails and access restrictions?
* To only allow authorised users access to certain data and information.
* To have a record/verifiable evidence of what has happened and what transactions have transpired.

1. Systems security software
   1. What types of security software should organisations run?

* Encryption software
* Antivirus software
* Firewalls
  1. Explain the nature of malware and phishing software
* **Malware-** Computer designed program to have harmful effects on an individual/groups data and files.
* **Phishing-** A way of gaining personal information such as credit card numbers and passwords through sending various emails purporting to be from reputable companies.
  1. Explain the nature of a firewall?
* A program or device that acts as a barrier to keep destructive elements out of a network or specific computer.

1. Encryption
   1. What does encryption involve?

* It’s the process of converting information or data into a code, especially to prevent unauthorised access.
  1. What protocols are used for encryption?
* **TLS and SSL**- These are cryptographic protocols that provide communications security over a computer network. The connection is private/secure because symmetric cryptography is used to encrypt the data transmitted.
  1. What is hashing?
* A method of encryption that can be used to encrypt the contents of databases inside fields; a method of protecting passwords by taking a variable length password and creating a cryptic, fixed length password from it by generating a salt value.